The Value of Identifying and Recovering Lost GN&C Lessons Learned: Aeronautical, Spacecraft, and Launch Vehicle Examples

Cornelius J. Dennehy[1]
NASA Engineering and Safety Center (NESC)

Steve Labbe[2]
NASA Johnson Space Center, Houston, TX, 77058

Kenneth L. Lebsock[3]
Orbital Sciences Corporation, Technical Services Division, Greenbelt, MD 20770

Within the broad aerospace community the importance of identifying, documenting and widely sharing lessons learned during system development, flight test, operational or research programs/projects is broadly acknowledged. Documenting and sharing lessons learned helps managers and engineers to minimize project risk and improve performance of their systems. Often significant lessons learned on a project fail to get captured even though they are well known 'tribal knowledge" amongst the project team members. The physical act of actually writing down and documenting these lessons learned for the next generation of NASA GN&C engineers fails to happen on some projects for various reasons. In this paper we will first review the importance of capturing lessons learned and then will discuss reasons why some lessons are not documented. A simple proven approach called 'Pause and Learn' will be highlighted as a proven low-impact method of organizational learning that could foster the timely capture of critical lessons learned. Lastly some examples of "lost"GN&C lessons learned from the aeronautics, spacecraft and launch vehicle domains are briefly highlighted. In the context of this paper "lost" refers to lessons that have not achieved broad visibility within the NASA-wide GN&C CoP because they are either undocumented, masked or poorly documented in the NASA Lessons Learned Information System (LLIS).

Nomenclature

ACS	=	Attitude Control Subsystem
AGS	=	Ascent Guidance System
AKM	=	Apogee Kick Motor
CoP	=	Community of Practice
CV	=	Controlled Variable
FCS	=	Flight Control System
FEM	=	*Finite Element Model*
FIB	=	Failure Investigation Board
GN&C	=	Guidance, Navigation, and Control
IFA	=	In-Flight Anomaly
KM	=	Knowledge Management

[1] NASA Technical Fellow for GN&C, NASA Goddard Space Flight Center, Mail Code 590, Greenbelt, MD 20711, USA, 240-687-9077, cornelius.j.dennehy@nasa.gov, Member AIAA
[2] Constellation Chief Engineer, NASA Johnson Space Center, Houston, TX, 77058, USA, 281-483-4656, steven.g.labbe@nasa.gov
[3] Senior Engineering Manager, Orbital Sciences Corporation, 7500 Greenway Center Drive, Ste. 700, Greenbelt, MD 20770, USA. ken.lebsock@nasa.gov, Senior Member AIAA

LLIS	=	Lessons Learned Information System
NASA	=	National Aeronautics and Space Administration
NEN	=	NASA Engineering Network
NESC	=	NASA Engineering and Safety Center
OAE	=	Orbit Adjust Engine
OML	=	Outer Mold Line
PTO	=	*Port Transducer Unit*
RCS	=	Reaction Control Subsystem
REA	=	Reaction Engine Assemblies
PaL	=	Pause and Learn
P&I	=	Proportional and Integral
TDT	=	Technical Discipline Team
TVC	=	*Thrust Vector Control*
WTR	=	Western Test Range
ΔV	=	Change-in-Velocity

I. Introduction

Few within the aerospace community doubt the importance of identifying, documenting and widely sharing lessons learned during the execution of system development, flight test, operational or research Programs/Projects. Managers and engineers alike acknowledge they can minimize their project risks and improve performance of their systems by a careful examination of NASA's detailed record of successes and failures. It is especially valuable when lessons learned can be leveraged by managers and engineers alike on new development projects to help overcome the project team's unfamiliarity with previously identified technical pitfalls and challenges.

A. The Challenge of Identifying, Documenting, and Sharing Lessons Learned

NASA Procedural Requirement (NPR) 7120.6 established the requirements for the collection, validation, assessment and codification of lessons learned submitted by individuals, NASA directorates, Programs and Projects, and any supporting organizations and personnel. Within the Agency the responsibility for overseeing and managing lessons learned belongs with the NASA Chief Engineer. One of the NASA Chief Engineer's primary tools to execute this responsibility is the NASA Engineering Network (NEN), which houses the Lessons Learned Information System (LLIS). The Office of the Chief Engineer (OCE) also utilizes the Academy of Program/Project and Engineering Leadership (APPEL) and their ASK Magazine to communicate real world engineering experiences/lessons as a key element of the NASA engineering workforce professional development. The OCE's basic underlying guiding principle is to see to it that lessons learned will be infused into Programs and Projects at key decision points. It is expected that Program/Project Managers will lead this infusion process and, together with the NASA Chief Engineer, they will find ways to embed the lessons directly into their individual design & development processes.

Identifying and capturing Guidance, Navigation and Control (GN&C) lessons learned is a demanding task under the best of circumstances; it is all the harder still to go about documenting lessons learned that occurred 5-15 years in the past. Ideally individuals and teams should document their lessons learned while they are still fresh in their mind and the team is functioning and intact. As Goodman (Ref. 1) has pointed out the collecting, researching, identifying, and documenting lessons learned that will be useful to current and future management and engineering personnel is not always a straightforward task. Reference I presents lessons learned and best practices concerning the research and documentation of technical and organizational lessons learned. It is intended to enable organizations to initiate or improve lessons learned research and documentation efforts.

Past studies by the Rand Corporation and the Government Accounting Office have concluded that NASA needed better mechanisms for broadly sharing lessons learned across the Agency. When surveyed during these studies engineers responded that while they were very or somewhat knowledgeable about lessons generated by their own programs and centers, they know much less about lessons generated elsewhere. The RAND study confirmed concerns that NASA had not heeded past lessons learned. The purpose of the study was to provide guidance on practices that reduce risk and improve the performance of next-generation spacecraft by including an examination of

NASA's successes and failures in building spacecraft both before and after implementing the faster, better, cheaper approach. The RAND study (Ref. 2), conducted in 2000, identified the top ten sources of failures in NASA programs and reported that a significant source of error has been the failure of NASA to incorporate lessons previously learned and consistently apply them. The GAO study (Ref. 3), conducted in 2003, of selected NASA's program/project managers revealed weaknesses in the collection and sharing of lessons learned agency-wide. While some lessons learning does take place, the GAO study found that lessons are not routinely identified, collected, or shared by programs and project managers. Respondents reported that they are unfamiliar with lessons generated by other centers and programs. In addition, many respondents indicated that they are dissatisfied with NASA's lessons learned processes and systems. Managers also identified challenges or cultural barriers to the sharing of lessons learned, such as the lack of time to capture or submit lessons and a perception of intolerance for mistakes. They further offered suggestions for areas of improvement, including enhancements to LLIS and implementing mentoring and "storytelling," or after-action reviews, as additional mechanisms for lessons learning.

NASA has responded to that criticism and has taken steps to improve the way it captures and shares information by developing an internal business strategy focused on 'knowledge management'. In this context Knowledge Management (KM) is defined as the way that the NASA engineering organizations create, capture, and reuse knowledge to achieve their objectives. NASA is still striving to be an effective 'learning organization' and has established teams and processes to coordinate KM activities at NASA's centers, and initiated several novel information technology pilot projects.

The fundamental importance of being a learning organization was emphasized by both the NASA Chief Engineer and the NASA Chief of Safety and Mission Assurance (S&MA) in a letter directive to the NASA Center Directors as well as the Engineering Directors and the S&MA Directors at all the NASA centers. In their letter (see Ref. 4), Mike Ryschkewitsch and Bryan O'Connor, state the following:

"We are writing to request your active participation in addressing an issue of critical importance to the long-term health of NASA. NASA makes significant investments in the intellectual capability of our workforce, but all too often we do not make time available to capitalize on these investments. Our technical workforce possesses a depth and diversity of expertise that is second to none in the world, yet we leverage only a fraction of our capacity to share our knowledge and lessons learned with each other. At the senior leadership level, we trust that grassroots efforts will take care of this, but we do not expend enough personal effort supporting these activities from the top.

This is not a new concern. In 2003, the Columbia Accident Investigation Board concluded that "NASA' s current organization...has not demonstrated the characteristics of a learning organization."1 Many high reliability organizations wrestle with this issue. The recent news about the "Spirit of Kansas" B-2 stealth bomber crash, where a technique learned by some flight and maintenance crews but not others probably would have prevented the accident, is a dramatic reminder that knowledge sharing is not "nice to do" — it is "must do."

Ryschkewitsch and O'Connor go on in their letter to encourage the senior management and technical leadership within NASA to institutionalize the learning process within their organizations and to and to take the initiative to improve NASA s performance as a learning organization.

One such recently implemented OCE initiative is the establishment of online engineering discipline communities of practice (CoPs). For example, an Guidance, Navigation and Control (GN&C) engineering online community (see Ref. 5) has been created which directly supports NASA's goal of being a world-class learning organization by facilitating knowledge sharing, especially lessons learned, between GN&C discipline engineers across the agency. Instituting an online site that encourages GN&C engineers from all centers to openly share their experiences, both positive and negative, helps to address the problem that many engineers are unfamiliar with the lessons learned on other Center's projects. This is a very positive first step but clearly NASA still needs to continue to create an environment and implement mechanisms to improve the 'cross-pollination' of GN&C engineering experiences across all the Agency's Centers. All too often a lesson learned at one Center remains exclusively within that center-level 'stovepipe' and unless it is entered into the NASA LLIS database, it is not visible to other members of the GNC CoP working at the other nine NASA Centers. With the ten (10) NASA centers spread around the country, there are very few built-in opportunities for face-to-face cross-pollination among the GN&C engineering technical workforce. The NESC is implementing measures to compensate for this geographical separation and to create technical forums for cross-Center interaction. The NESC is sponsoring, organizing , and hosting specific technical

workshops such as the Orion/Mars Science Lab Entry, Descent and Landing (EDL) Workshop held in March 2009 at LaRC and the NASA GN&C Workshop held in Cambridge, Massachusetts in June of 2010.

B. Leveraging the 'Pause and Learn' Approach to capture Lessons Learned

The rigorous "Post-Mortems" that are typically conducted after an anomaly, mishap or failure certainly document key findings, provide recommendations and offer detailed and comprehensive insights. While they ultimately provide a very valuable product these rigorous post-mortem only occur reactively after the 'damage' is done (i.e., the occurrence of a major mishap or failure) and can often require several months, to over a year in some cases, to be completed. Furthermore the product created is typically a lengthy report documenting a wide-scope look at the event which, frankly, few practicing individual-contributor engineers ever see or read.

In order to stimulate timely and near-continuous learning before any serious consequence occur NASA has, over the last few years, instituted an effective quick reaction method of identifying, communicating, and documenting localized Program or Project team knowledge. NASA's 'Pause and Learn' (PaL) approach (Ref. 6) is similar to other methods successfully adopted and practiced by many government and corporate 'learning' organizations such as the U.S. Army, Shell Oil, IBM, Fidelity Investments, and Harley Davidson. A PaL session is a method for reflecting and transferring individual lessons from a specific project event among fellow team members. Team members meet behind closed doors, take off their official Program or Project "hats" for a brief period, and look back on a recent event to gain a more thorough understanding of what has happened, and why. NASA has found this to be an effective low-impact way to: a) identify and spread local best practices, b) implement on-the-spot individual and team learning, c) build a team approach to problem solving, d) build team morale, and e) increase likelihood of project success. An informal PaL session typically explores many issues but two key questions the team focuses on are: 1) What did we learn from this event or situation?, and 2) What should we change? The NASA PaL process does not create formal reports as an output product. However, the authors are suggesting here that, under the right circumstances and in the right situations, the basic information presented and discussed amongst the team in a given PaL session could easily be taken and used in a straightforward manner to formulate new lessons learned for submittal to the NASA LLIS database. Alternatively, a PaL-like informal team meeting approach could be instituted with the sole purpose of identifying and concisely documenting lessons learned as they occur.

C. The Need to Recover 'Lost' GN&C Lessons Learned

It is the authors belief that overall the knowledge sharing framework has improved over the past several years allowing for better communication of lessons learned. It is hoped that the GN&C engineers at NASA, especially the early-career engineers, will take notice of the new resources being made available to them and take full advantage of these enhancements in KM systems and processes.

But one can't easily review a lesson learned that is "lost" and has never been captured in one form or another. There are several reasons and factors that tend to limit the capture of useful lessons learned. Although the GN&C engineering practitioners across the Agency are often reminded of the importance of (and in some organizations, the requirement of) applying relevant lessons learned to their individual day-to-day tasks, there is little in the way of specialized education, training, and materials made available to help those engineers do a better job of managing critical knowledge and capturing lessons learned.

All too often at the end of project (especially when it is abruptly terminated) there is neither the management mandate, nor sufficient time or budget set aside for GN&C engineers to first identify all their lessons learned and to then document them for future dissemination within the Community of Practice (CoP).

Some examples of "lost" lessons learned, taken from the aeronautics, spacecraft and launch vehicle domains, are briefly highlighted in the next four sections of this paper. In Section II the case of the US Air Force B2-bomber crash mentioned above is discussed as an example of the negative results that can happened when either critical technical information is not captured in a process or procedure or when a Lesson Learned report is not written and

shared. The second example, presented in Section III, addresses an unanticipated and anomalous 360-degree rollover event which occurred on the X-38 flight test program. Several significant lessons learned emerged from the post-anomaly investigation but were never formally captured for posterity in the NASA LLIS. The two last examples to be cited in this paper of 'lost' GN&C-related lessons learned come from two different commercial endeavors that took place in the mid-1990's: the Landsat-6 commercial remote sensing spacecraft failure in 1993 (Section IV) and the Conestoga commercial launch vehicle failure in 1995 (Section V). The significant GN&C-related lessons learned from these two commercial-sector failures have neither achieved broad visibility within the NASA-wide GN&C CoP nor have they been captured in the NASA LLIS.

The intention of the authors is to tangibly demonstrate that there is valuable GN&C knowledge missing from the NASA LLIS. Knowledge, that with a modest amount of Project/Program data mining and perhaps a few short interviews with the key personnel involved, can be concisely documented. It is a difficult task to attempt to reconstruct complex event well after fact and without the benefit of having a technical interaction with the full Program/Project team while their memories of what happened are still fresh. This retro-active process of recovering 'lost' lessons learned is not optimal but it does take the first step in filling some key knowledge gaps.

II. B-2 Bomber Lessons Learned (February 2008)

The B-2 stealth bomber crash alluded to in Section I above illustrates a fundamental message the authors wish to send with this paper, albeit the source is from a non-NASA culture: the failure to capture and broadly share critical system knowledge in a timely and concise "Lessons Learned" report can have catastrophic consequences.

The B-2 "Spirit of Kansas" crash occurred on February 25th, 2008 at Andersen Air Force Base in Guam. Seventeen seconds after takeoff the bomber's crew was unable to control the aircraft and its left wing struck the ground. Before take-off, the plane's computers had called for an internal Air Data System (ADS) calibration. Because of Guam's humidity, there was moisture in the air data sensors during calibration. During taxi for takeoff, the moisture evaporated. The now mis-calibrated ADS sent skewed data to the Flight Control System (FCS), which in turn commanded the aircraft nose up to pitch up 30° upon takeoff. Unable to regain control of the vehicle, the B-2's two-member crew ejected safely just barely before the plane crashed and burst into flames (see Figure 1). The subsequent Air Force investigation concluded that an underlying root cause of the $1.4B aircraft being totally destroyed was because critical information was not communicated effectively (Ref. 7 and Ref. 8)

The brief history behind this unfortunate incident is as follows. During the B-2's 2006 deployment in Guam, the extremely humid environment required frequent ADS calibrations. Line maintenance technicians telephoned the B-2 manufacturer technical representatives to ask advice on this new environmental issue. Support engineers recommended using the aircraft's pitot heater to dry the Port Transducer Unit's PTU's be-fore calibrating the ADS. Pitot heat is supplied to prevent icing of pitot-static sensors in flight; extensive ground use could overheat and damage the pitot-static system. Several maintenance technicians used pitot heaters successfully to dry moist PTU's and accurately calibrate the ADS, but this technique was neither formalized by a change to the appropriate technical order (i.e., operational procedure) nor captured in a "Lessons Learned" report. The post-crash investigation determined that only some of the ground crews and pilots working with the B-2s during their 2007-2008 deployment were aware of the ADS's sensitivity to moisture and the pitot heat procedural workaround (Ref. 14 and Ref. 15).

Figure 1: The Crashed B-2 Bomber "Sprit of Kansas" at Andersen Air Force Base

III. X-38 Drop Test Lessons Learned (November 2000)

The X-38 Program was originated in 1995 as a technology demonstrator project at the Johnson Space Center (JSC). It was quickly focused to demonstrate technology and concepts for a Crew Return Vehicle (CRV) for the International Space Station (ISS). During the course of the program, the X-38 evolved from technology demonstrator to CRV prototype to its ultimate configuration as a demonstrator that would be modified after its initial test flight into the first operational CRV. The X-38 project was a joint effort between the Johnson Space Center, Houston, Texas (JSC), Langley Research Center, Hampton, Virginia (LaRC) and Dryden Flight Research Center, Edwards, California (DFRC) with the program office located at JSC. A contract was awarded to Scaled Composites, Inc., Mojave, California, for construction of the X-38 test airframes. The first vehicle was delivered to the JSC in September 1996. The vehicle was fitted with avionics, computer systems and other hardware at Johnson. A second vehicle was delivered to JSC in December 1996.

On 2 November 2000 the X-38 prototype vehicle V131R, which was an 80% scale version of the Crew Return Vehicle (CRV), conducted its first drop test, or Free Flight One (FF1), over California's Mojave Desert near the NASA Dryden Flight Research Center. As depicted in Figure 2 the B-52 carrier aircraft dropped the V131R prototype at M=0.6 at an altitude of 11,000 m (36,500 ft). Immediately following its release from the B-52 the V131R lifting body made an "unplanned" 360-degree right roll around the velocity vector after it was jettisoned. The vehicle paused at 180° and there was over 1 second of fully inverted flight (Figure 2). Fortunately a safe landing was accomplished with minimal structural damage and the vehicle was recovered intact which greatly supported the investigation of this In-Flight Anomaly (IFA).

The cause of the yawing moment[4] IFA was investigated and subsequently traced to two major items: 1) the fact that the asymmetric aerodynamic roll & yaw moments far exceeded predictions, and 2) the Flight Control System (FCS) performance margin was insufficient to trim out large aero moments. The V131R vehicle's yaw moment was four times the preflight Aerodynamic DataBase (ADB) uncertainty value. The rudder trimmed at 2-3° instead of zero degrees. So, when with the uncharacterized larger aerodynamic yawing moments combined with a Flight Control System (FCS) that was purposefully biased for stability over performance one can see how the resulting vehicle rollover during the initial flight test could occur.

[4] For lifting bodies, yaw translates directly into roll. Therefore the unexpectedly large aerodynamic yaw moment primarily caused the 360° rollover.

Figure 2: B-52 Carrier Aircraft Drop of V131R X-38 Prototype

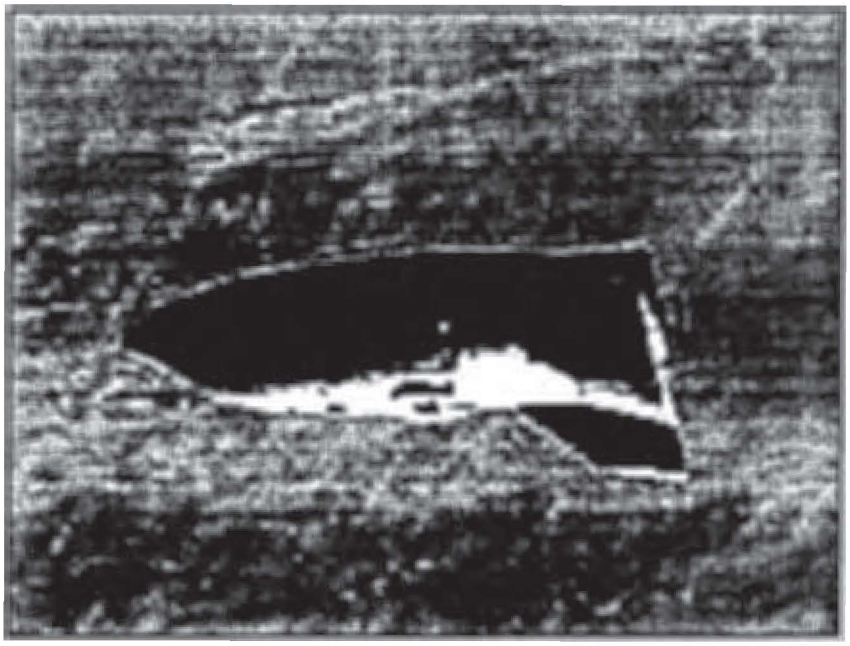

Figure 3: V131R X-38 Prototype in Inverted Flight during In-Flight Anomaly

As a cost & schedule savings, V131R airframe was fabricated in a low-cost manner from fiberglass materials. As described in Reference 9, this resulted in manufacturing discrepancies in the airframe Outer Mold Line (OML) geometry typical of a fiberglass construction. A moderately accurate laser survey of the OML was performed prior to the FF1 test. The laser survey results provided evidence of these OML geometry discrepancies as well as a left-to-right asymmetry (see Figure 4). Figure 3 depicts the deviation between the measured as-built fiberglass OML and

the specified dimensioned OML Computer Aided Design (CAD) drawings. The pre-drop Computational Fluid Mechanics (CFD) aerodynamic modeling and analysis was performed using an 'as built' OML CAD model reflecting the manufacturing discrepancies discovered by the laser survey. The X-38 Aerodynamics team did not consider these "bent airframe" and asymmetric base flow discrepancies to be significant. The V131R FF1 drop test clearly proved that assertion to be incorrect. When combined with a base asymmetric aerodynamic phenomenon, the built in vehicle asymmetry contributed to uncharacterized yaw and roll increments.

Following the yawing moment IFA higher accuracy photogrammetric measurement techniques were performed on the recovered V131R airframe. The geometric measurements obtained from the photogrammetric survey were used to develop new CAD models of the as built vs. specified geometries. These updated CAD models were then used to perform updated CFD analyses. This post-drop analysis more accurately estimated the asymmetric vehicle contribution to the yaw anomaly (~1/3 of the effect) which combined with the base asymmetry phenomenon to produce the un-modeled aerodynamic moments on V131Rs first flight.

Figure 4: V131R X-38 Prototype Pre-Drop Test OML Laser Survey Results (Deviation between the As-Built OML Dimensions and the OML CAD Dimensions)

The Multi-Application ControlH (MACH) was used as X-38 Flight Control System during free flight tests (Ref. 9). This advanced control system architecture (see Figure 5) was developed at Honeywell Research Center by Dale Enns & Dan Bugajski in early 1990's. MACH is a modular, nonlinear multivariable design approach which mixes classical control design with dynamic inversion. For the X-38 application the MACH FCS consisted of a blended implementation of inner-loop Dynamic Inversion (DI) plus the classical Proportional and Integral (P&I) control actions in the outer-loop.

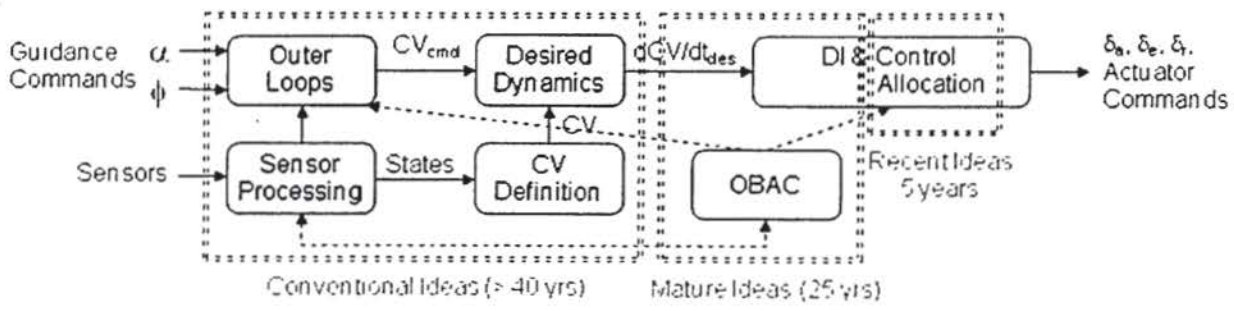

Figure 5. X-38 MACH Flight Control System Architecture

In the MACH architecture an Onboard Aircraft (OBAC) model was used to compute the expected dynamics during flight. Effectively the OBAC model provides automatic gain scheduling, eliminating multiple linear point designs. The expected nonlinear dynamics inverted to cancel from sensed dynamics. Effector commands are computed to produce linear, first order desired dynamics. The desired dynamics and outer command error loops protect against modeling error. An attractive feature of the MACH FCS architecture is that although it employs a different design process than classical methods the same classical verification approaches can be employed. The key aspects that the control system design focuses on are the selection of Controlled Variables (CV) and OBAC aerodynamics model.

The FCS design requirements had emphasized very robust stability over performance in the face of large aerodynamic database uncertainties. Given the desire for all test vehicles to remain stable despite all aerodynamic uncertainties and unknowns to ensure a good parachute deployment and vehicle recovery, the FCS design was biased toward greater stability margin at the expense of performance margin. There were therefore "fat" stability margins in the forward/effector and feedback/sensor loops. During the yawing moment IFA the V131R vehicle was stable during the entire roll, due to large stability margins, but had inadequate lateral performance to quickly stop the roll.

In addition to the aerodynamic problems it was found during the investigation that an undetected FCS flight software implementation error effectively reduced the roll channel error gain by half. Since this gain setting error mainly affected performance, stability margin comparisons between the design model and the implemented FSW did not reveal the gain error. In fact, even with the gain error, the FCS FSW was certified to meet all specifications and requirements. Step-response comparisons between the linear design models and the FSW that would have caught the error were not part of the existing pre-flight certification process, but were later added to the certification process. All subsequent certifications compared *both* the stability and performance metrics of the original FCS design models with the final FCS FSW. Post-FF1 analysis indicated that having the correct roll channel gain may have stopped roll at about 90° of rotation. The low outer loop Proportional & Integral gains on roll tracking error contributed to the low performance margin. The rudders responded slowly to the increasing roll and did not use all available deflection.

The FCS had been certified with the incorrect roll gain for the predicted aero uncertainties. The FF1 certification process involved 1500 Monte Carlo runs plus another 2628 deterministic simulation runs for a grand total of 4128 total runs. The deterministic simulations were intended to stress the FCS with preselected "bad" dispersion parameter sets. Nevertheless the certification process had failed to uncover the risk of roll-over. The ADB uncertainties did not bound actual asymmetric aerodynamics observed on FF1 (see Figure 6) and the certification process did not go beyond the established ADB uncertainties.

Based upon what the investigation into the causes of the FF1 roll-over incident there were several changes made in the both the aerodynamic database and in the FCS design itself. New values of Cl_0 & Cn_0 , the roll and yaw aerodynamic bias terms, both nominal terms and the uncertain terms, were incorporated into the ADB.

The original FCS was seriously 'under-gained'. Figure 7 depicts, in yellow, the FCS design modifications resulting form the IFA investigation (Ref. 9). The FCS modifications included included increased outer loop P&I gains to trade some stability margin for performance margin to meet new, tighter performance requirements. The loop gains were increased by a factor between 2X and 9X; the largest single gain increase occurred on the roll/yaw rate trim gain which was increased by a factor of nine (9). Figure 8 illustrates the greatly improved FCS roll axis step response performance achieved after the tuning up the FCS gains. Additionally, a sideslip approximation was added to the Controlled Variable (CV) with filtered lateral acceleration feedback. The FCS Onboard Aircraft (OBAC) model was based upon the off-nominal aerodynamics to maintain robust stability. Lastly anti-windup logic was added to CV integrator to improve the B-52 release transient response.

Changes were also made in the certification process for FF2, the second free-flight drop test. The new focus for FF2 certification was to "push" the aerodynamic uncertainties outside ADB and test the limits of the FCS. The asymmetric aerodynamics uncertainty was particularly targeted as a place to expand the uncertainty. The simulations employed for certification were divided into three categories:

Category 1: Core simulations => expected flight conditions + 3-sigma dispersions

Category 2: Investigation simulations => extreme flight conditions, well beyond 3-sigma dispersions

Category 3: Stress simulations => to test the limits of the FCS

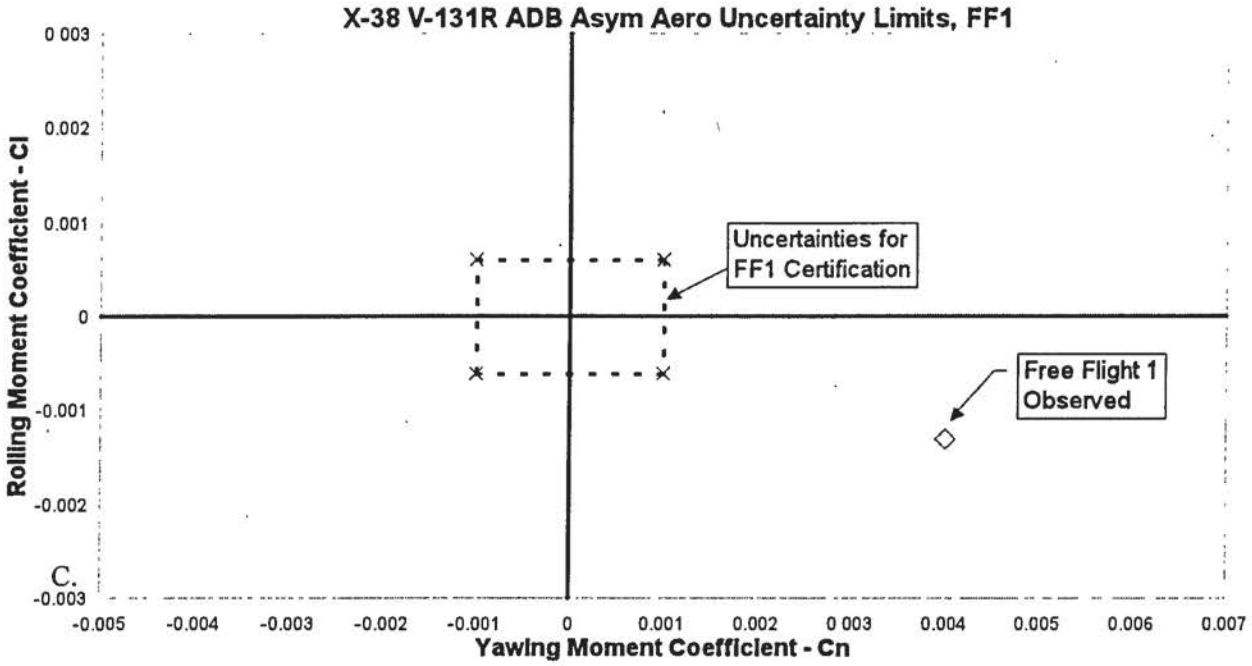

Figure 6. V131R FF1 Asymmetric Aerodynamics

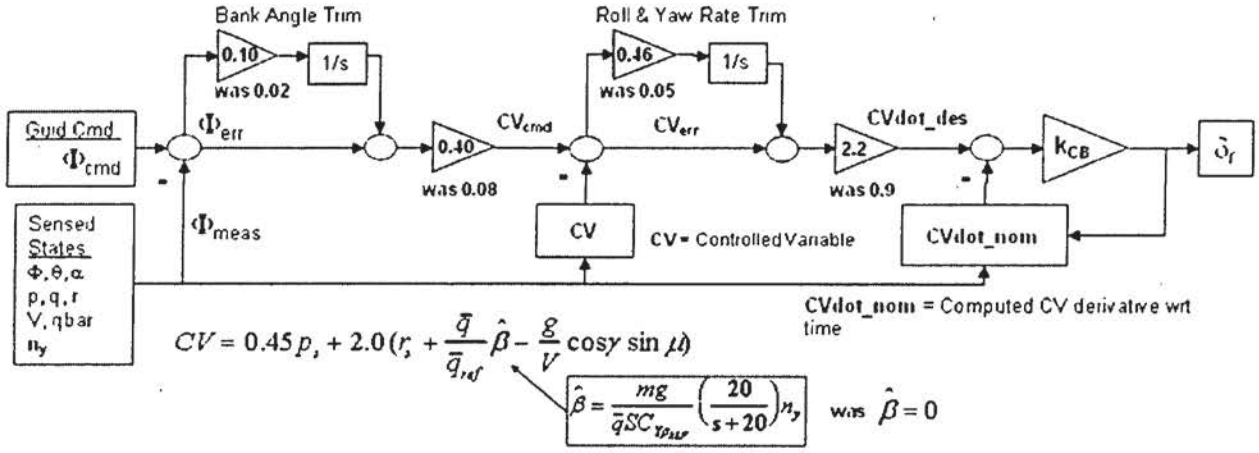

Figure 7. X-38 Flight Control System Modifications

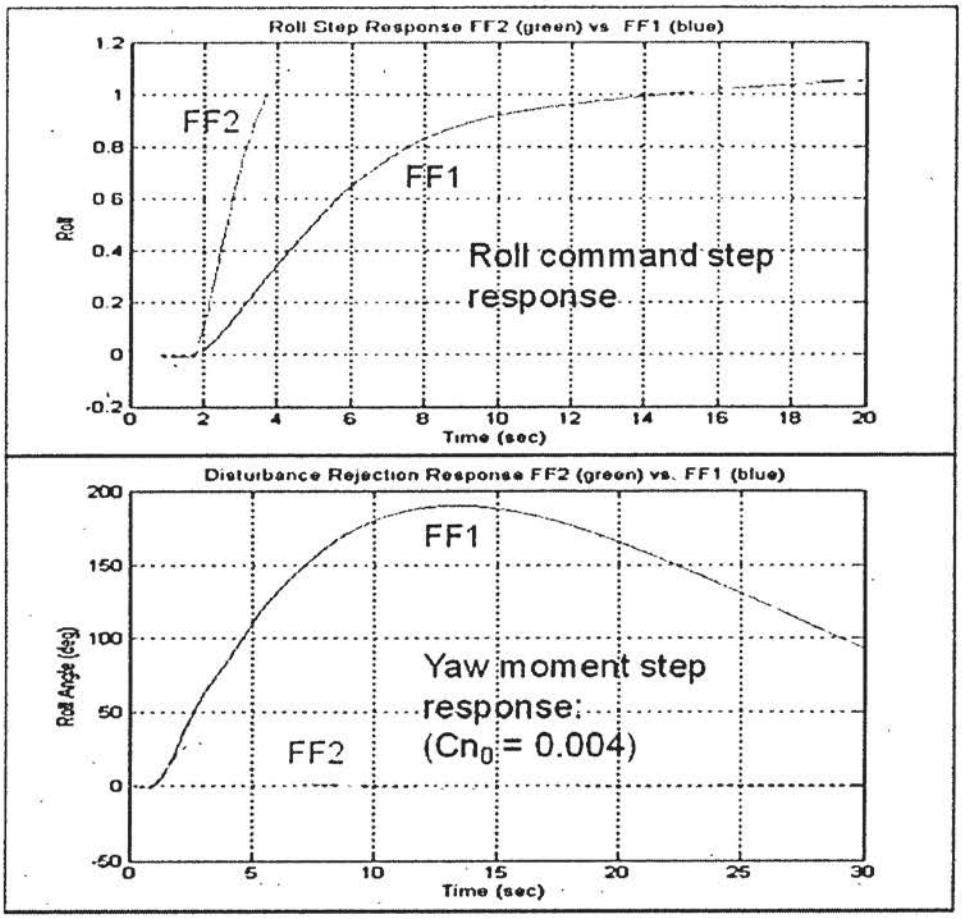

Figure 8. X-38 Flight Control System Roll & Yaw Step Responses

There were also modifications to the Monte Carlo simulation approach with uniform distributions, instead of Gaussian distributions, applied on some of the parameter dispersions. Additional Monte Carlo simulation runs were performed to examine FCS sensitivity to very large aerodynamic dispersions well beyond ADB uncertainties. Lastly there was a shift in certification philosophy to concentrate more upon Monte Carlo dispersed simulations than the deterministic simulations in which stressing dispersion parameter sets were pre-selected: 3100 Monte Carlo runs were performed plus 1918 deterministic runs for a grand total of 5018 total runs.

Independent Verification and Validation (IV&V) checks were also performed with separate NASA and contractor software groups (see Ref. 10). NASA and Honeywell engineers performed linear stability and performance analyses with independently created models for every FCS certification. Since both teams were using linear models, their cross-checks of FCS gain and phase stability margins and step responses typically matched closely. As part of their rigourus IV&V process the teams also compared the non-linear gain margins, determined using the final as-coded FSW, to the designed values of linear gain margins. These comparisons did not match as tightly as the linear-to-linear stability margins comparisons did, but this cross-check was suffiecnt to flag gross implementation or modeling errors in the FCS.

Looking back on this incident with 20-20 hindsight, one can see that a combination of inaccurate aerodynamic data and low FCS performance margin resulted in V131R FF1 roll-over. The improved ADB and FCS resulted in a nominal FF2 drop test where the maximum roll and pitch angles were within 1° of pre-test predictions.

So what are the lesson to be learned from the X-38 rollover? It appears there are at least five significant lessons learned emerging from the X-38 FF1 yawing moment IFA investigation. The five lessons learned that can be taken away from this incident and which should be widely shared within the GN&C CoP are:

X-38 LL #1

Test The OML Geometry You Fly / Fly The OML Geometry You Test: – Engineers must confirm, via sufficiently accurate test and survey methods, that the as-built geometry of the vehicle's OML matches, within some pre-established tolerance the OML structural CAD drawing dimensions. Small deviations in OML geometry can have significant impacts if not accounted for. Ensuring the OML is within specification, and/or that any out of tolerance deviations between the geometry specification and the as-built OML, must always be done. Performing this type of OML geometry confirmation testing is especially important prior to the first flight of a new generation of aereonautical vehicle and/or a one-of-a-kind aeronautical vehicle.

X-38 LL #2

Validate the OML Geometric Database Model Used for CFD Modeling and Analysis: Establish a plan to ensure the OML geometric database model used in CFD modeling and analysis evolves, over the course of multiple design cycles, from an initial idealized smooth shape to the as-built shape incrementally incorporating relatively small but potentially influential OML structural/geometric modifications. A high fidelity verification test should be part of the overall plan to ensure a valid OML data base. Prior to first flight ensure that geometric CFD and Wind Tunnel Test (WTT) models are within the pre-established sufficiently small tolerances requirements necessary to generate an acceptable data base.

X-38 LL #3

Understand Flight Control System Sensitivity to Uncertianty:
The flight control system designer should always determine uncertainty sensitivity of the flight control system

X-38 LL #4

Strike a Reasonable Balance Between Flight Control System Stability Robustness and Performance Margins
The flight control system designer should always balance stability margin and performance margin

X-38 LL #5

Carefully Consider Bandwidth Allocation in a Multi-Loop Flight Control System:
The flight control system designer should carefully consider bandwidth allocation in a multi-loop system. The final FCS design should typically set the ratio of inner loop bandwidth to outer loop bandwidth to be in the range between 2-to-1 and 4-to-1.

Note, for the record, both the X-38 LL #1 and the X-38 LL #2 lessons learned defined above are in fact mentioned in Reference 10 (Page 39 of that report) but their mention is so deeply buried in this large summary report it is not likely to easily come to the attention of practicing GN&C engineers.

IV. LANDSAT-6 Commercial Remote Sensing Satellite Lessons Learned (October 1993)

The Landsat series of Earth remote-sensing satellites dates back to 1972. The mission of the Landsat Program is to provide repetitive acquisition of moderate resolution multispectral data of the Earth's surface on a global basis. Landsat-6 was the sixth spacecraft in the series and was unique in that it was developed commercially whereas NASA had been responsible for the development and launch of all the preceding Landsat satellites. With the passage of Public Law 98-365, the "Land Remote Sensing Commercialization Act of 1984", the National Oceanic and Atmospheric Administration (NOAA) was directed to delegate management of the Landsat 4 and 5 satellites and their data distribution to the private sector. In addition, NOAA was to pursue procurement of future remote sensing Landsat products and services from the private sector. In 1985, NOAA solicited bids to manage the existing Landsat satellites and to build and operate future systems. The Earth Observation Satellite Company (EOSAT), a joint venture between RCA and Hughes Aircraft, won the competitive bidding process in August 1984 and took over

operation of the Landsat system on September 27, 1985. The Landsat-6 development was managed by EOSAT under the oversight of NOAA with funding from the Department of Commerce. A technical overview of the Landsat-6 spacecraft is provided in Reference 11 while Figure 9 shows the spacecraft during the development process.

The Landsat-6 spacecraft was launched on 5 October 1993 on a Titan-II booster. Throughout ascent all telemetered data from the Titan-II was nominal. No Landsat-6 spacecraft real-time telemetry was available during ascent due to an S-band frequency conflict with Titan-II booster. The entire ascent phase was planned to take approximately 40 minutes at which point the Ascent Guidance System (AGS) would "hand over" control to spacecraft's Orbit Mode attitude controller. The telemetry data indicated that spacecraft separation from the booster occurred at the nominal time and place. All expectations were that contact with the spacecraft would be nominally established at the first ground station (Kiruna, Sweeden) approximately seventy (70) minutes after launch. This first contact with Landsat-6 was never established and subsequent attempts to locate the spacecraft were futile. The inability to make contact with the Landsat-6 spacecraft coupled with reports from other assets indicating reentry events downrange from the observed Titan-II booster stage reentry events subsequently led the the conclusion that the spacecraft had not achieved orbit following separation from the Titan-II.

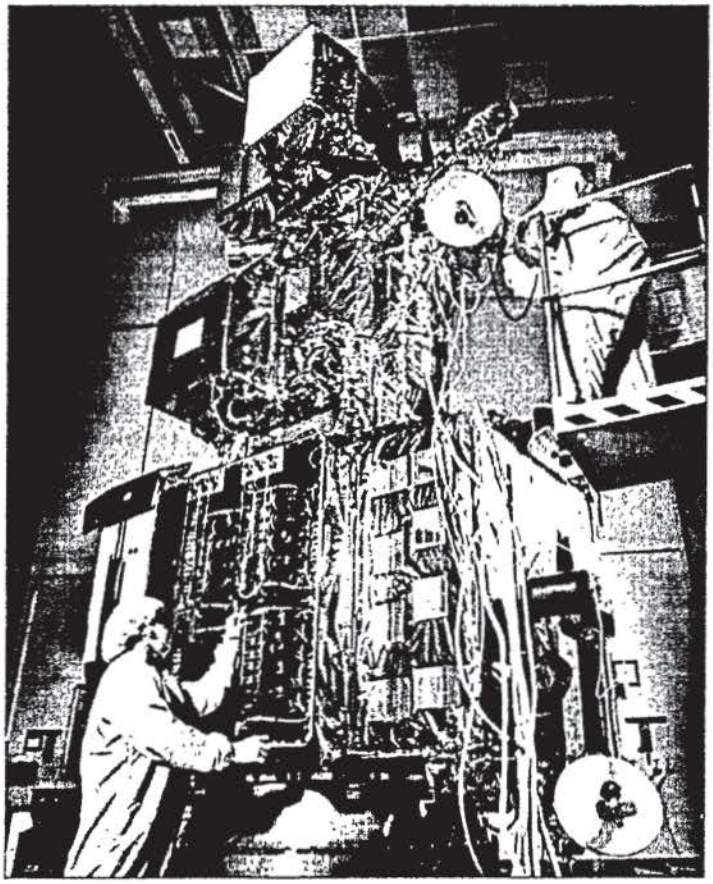

Figure 9. Landsat-6 Earth Remote Sensing Spacecraft During Development

The Landsat-6 failure investigation concluded that the spacecraft experienced a rupture in its Reaction Control Subsystem (RCS) hydrazine manifold. This ruptured hydrazine manifold rendered the spacecraft's Reaction Engine Assemblies (REA's) useless because the propellant could not reach the engines. The function of the four (4) 100-lbf REA's was to provide attitude control torques to adequately stabilize the spacecraft during the firing of it's solid-fueled Apogee Kick Motor (AKM). The Landsat-6 design employed a STAR-37XFP solid rocket AKM internal to

the spacecraft to provide the last increment of orbital insertion velocity needed for Landsat-6 to attain its 705-km circular polar Sun-synchronous mission orbit. This was a similar orbit insertion strategy utilized many times before by the Landsat-6 spacecraft contractor on the DMSP and TIROS military and civilian meteorological spacecraft in which the spacecrqft essentially serves as the third stage of the launch vehicle using AGS to navigate, guide and control the insertion into the mission orbit.

The Landsat-6 Attitude Control System (ACS) was designed to accommodate the anticipated significant disturbance torques that are typically generated during the firing of AKM solid rocket motors. However lacking the control authority of the REA's to maintain stable attitude control the spacecraft entered an un-controlled tumble during the AKM firing event. Consequently the spacecraft did not accumulate a sufficient Delta-Velocity (energy) from the AKM firing to attain an orbit about the Earth. The spacecraft re-entered the atmosphere south of the equator approximately 30 minutes after liftoff. The reentry of the spacecraft was validated by both a lack of a signal over the Kiruna ground station and the observations of other national assets.

The failure investigation discovered that although it was very similar to the heritage DMSP and TIROS spacecraft designs the Landsat-6 spacecraft required some mission unique modifications to its RCS design. These modifications altered the heritage of the RCS subsystem. The use of the STAR-37XFP AKM to provide the post-separation ΔV to attain the mission orbit traced back directly to the DMSP/TIROS heritage, as did the use of the four 100-lbf-thrust REA thrusters for stabilization and attitude control during the AKM burn. However modifications were needed to satisfy both the unique Landsat-6 mission level orbit maintenance requirements and the range safety requirements imposed by the Western Test Range (WTR) on Landsat-6. The first significant modification was to incorporate four (4) 1-lbf hydrazine Orbit Adjust Engine (OAE) thrusters into the Landsat-6 Reaction Control System (RCS) design to provide the ΔV for orbit maintenance. The second significant modification was to include two (2) Normally Closed pyrovalves to physically isolate the REA & OAE thruster manifolds from hydrazine until after liftoff. The WTR range safety office required the REAs to be 'dry' at liftoff unlike the DMSP/TIROS heritage practice of launching those spacecraft with their REA's being 'wet' with the hydrazine propellant. Although it was not fully appreciated prior to launch by the Landsat-6 System Engineering, Propulsion, and GN&C engineers these two modifications, one driven by a key mission requirement and the other driven by range safety considerations, fundamentally altered DMSP/TIROS RCS subsystem heritage.

The investigation by the Landsat-6 Failure Investigation Board (FIB) was severely constrained by a total lack of spacecraft telemetry but they did assemble and review all the available flight and ground test data which included the following: a) ground radar data, b) launch vehicle telemetry data including both structural and inertial guidance system accelerometer data, c) re-entry data and d) pyrovalve hot fire testing in a Landsat-6 RCS mockup. The FIB focused much of their attention on a detailed consideration of the time-dependent sequence of RCS operational events that occurred shortly before and directly following the separation of the Landsat-6 spacecraft from the Titan-II launch vehicle. This sequence of events is as follows:

1. Venting of "downstream" helium for 0.5 sec.
2. Normally Closed pyrovalve #1 fired
3. Normally Closed pyrovalve #2 fired 1 second after pyrovalve #1
4. Titan-II/L6 spacecraft separation
5. Short REA burn to impart separation velocity to L6
6. AKM ignited
7. REAs pulsed on to control attitude during AKM burn
8. AKM burn completed
9. Final velocity trim burn using REAs
10. Normally open pyrovalve fired to seal off REAs

The Landsat-6 FIB, after completing its review of the available data and considering the relative likelihood of multiple possible failure scenarios, concluded the Landsat-6 spacecraft experienced a rupture in the RCS hydrazine manifold. This rupture was caused by explosive detonation of hydrazine partly due to the 'water hammer' effect experienced in the RCS manifold after the firing of normally closed pyrovalve #1. This led to a condition in which there was hydrazine present on both sides of pyrovalve #2 prior to its firing. It was envisioned that hot gas 'blow-by' occurred when the normally closed pyrovalve #2 fired one second after pyrovalve #1 causing a frothy mix of hydrazine bubbles and trapped air to adiabatically detonate. The ruptured hydrazine manifold rendered the

spacecraft's REAs useless since propellant could not reach those engines. Without the stabilizing attitude control torques from the REAs the spacecraft tumbled uncontrollably during the subsequent AKM burn. Consequently the spacecraft did not accumulate sufficient ΔV (energy) from the AKM firing to attain Earth orbit and it re-entered Earth's atmosphere south of Equator approximately 30 minutes after liftoff.

The Landsat-6 Failure Investigation Board (FIB) concluded that the complete mission loss of the Landsat-6 spacecraft was due to over-reliance on heritage, and associated lack of propulsion subsystem testing, which led to hydrazine manifold rupture due to a detonation event triggered by pyrovalve activation. The details of the Landsat-6 failure investigation are contained in Reference 12. The FIB also observed that the modifications to DMSP/TIROS RCS subsystem heritage design were not fully appreciated at system level and there was a prevalent common view of the RCS as a low-risk "heritage" implementation. This view led to only limited modeling & test of the integrated RCS design. It was also pointed out that the Landsat-6 Project experienced several programmatic cost and schedule impacts resulting in the engineering team being either drastically ramped down or completely taken off the project. Therefore the RCS engineering lacked continuity and suffered from fractionated engineering support due to these programmatic starts & stops.

So what are the lessons to be learned from the Landsat-6 spacecraft failure? It appears there are at least four (4) lessons learned that can be taken away from the Landsat-6 experience that should be widely shared with the GN&C CoP:

LANDSAT-6 LL #1

Challenge the Validity and Viability of Heritage Designs

Don't take the apparent attractiveness of heritage designs on face value. Beware of an over-reliance on GN&C and Propulsion hardware, software or operational heritage. System Engineering should re-evaluate all proposed heritage systems in light of any potential or actual changes/differences in all mission requirements, mission applications and operational environments. Heritage designs, components, and systems must 'earn' their way onto the spacecraft. Spend the time to analyze and fully appreciate the cost/schedule/performance/interface/operational/risk impacts of any modifications to heritage designs. Don't simply assume heritage implementations to be low risk.

LANDSAT-6 LL#2

Ensure the Availability of Spacecraft Telemetry to Monitor Critical Launch and Ascent Events

Ensure that there is sufficient GN&C and Propulsion engineering telemetry down-linked, processed, and made available to monitor performance, diagnose anomalies, during the critical launch, ascent and early on-orbit operations phases when potential loss-of-mission failures can occur.

LANDSAT-6 LL #3

Perform modeling, analysis & test of integrated GN&C/RCS Systems

Develop a plan for sufficient modeling, analysis, and hardware testing of the integrated GN&C and RCS system interfaces, interactions, performance, and mission-critical time-sequenced operational sequences. Perform Hardware-in-the-Loop (HITL) testing to verify proper/expected HW/SW interactions in all operational modes, during mode transitions and all mission critical events. Understand all inter-dependencies and factor that information into the system-lelve risk analysis.

LANDSAT-6 LL #4

Avoid the Pitfall of Fractionated Engineering

To the maximum extent possible maintain the same engineering team during the conceptual design, detailed design, development and operational phase of a Program/Project. Develop plans and processes to ensure engineering workforce continuity and to compensate for key engineering personnel transitions. Implement sufficient measures to capture and clearly document the knowledge and experience of engineers leaving the program/project for future reference.

V. Conestoga Commercial Launch Vehicle Failure (October 1995)

The mission of the Conestoga commercial launch vehicle was to place the Multiple Experiment Transporter to Earth Orbit and Return payload (METEOR 1, formerly the Commercial Experiments Transporter, COMET 1) into Low

Earth Orbit along with its fourteen (14) on-board microgravity experiments. The METEOR 1 transporter was to be a recoverable payload, designed for on-orbit microgravity experiments advancing commercial applications of materials processing and medical research. The launcher and the spacecraft were designed and developed commercially by EER Space Systems over a five-year period with both NASA and private sector funding (see Ref. 13).

The Conestoga 1620 launch vehicle first stage consisted of a Castor 4A solid motor core, with six additional Castor 'strap-on' motors arranged symmetrically around the core. The set of six (6) strap-on motors consisted of four (4) Castor 4B solid motors with steerable nozzles plus two non-steerable fixed nozzle Castor 4A solid motors. A modern control theory based Linear Quadratic Regulator (LQR) controller was used to generate Thrust Vector Control (TVC) nozzle steering commands to the Castor 4B motors. Inertial sensor (i.e. rate gyroscope) feedback was used to stabilize and control the pitch axis and yaw axis atttiude. Roll control during first stage powered flight was accomplished by commanding differential nozzle steering. The LQR controller approach was adopted after an earlier classical control theory based Proportional, Integral and Derivative (PID) TVC control law design proved unable to handle the task of stabilizing the multiple flexible mode of the launch vehicle structure.

The maiden flight of the Conestoga 1620 launch vehicle, occurring on October 23, 1995 at NASA's Wallops Flight Faculty (WFF), resulted in a complete failure, with the vehicle going out of control at T+46 seconds at an altitude of 6 nm during first stage powered flight. While WFF routinely launches sub-orbital sounding rockets the Conestoga launch was the first orbital rocket launched out of that facility in 10 years. Figure 10 depicts both the Conestoga launch vehicle on its WFF launch pad (Figure 10a) and at the moment of liftoff (Figure 10b). At T+44.4 seconds the launch vehicle started a turn to the south and pitched down. The launch vehicles flight termination (self-destruct) system was commanded to fire the destruct explosive packages at T+46.202 seconds and the vehicle was disintegrated in midair (Figure 11). The destruct package failed to operate on two of the Castor 4 first stage motors but operated on the other four motors. At T+47.67 the destruct system destroyed a non-burning Castor 4B motor. The third stage Castor 4B motor and the fourth stage Star-48 kick apogee kick motor were not destroyed and they impacted in the ocean off Wallops Island.

The subsequent work of the Conestoga Mishap Investigation Board (MIB), consisting of EER Space Systems and NASA members) concluded that the rocket went out of control when one of its first-stage TVC engine nozzle steering actuators (on Castor 4 Motor #6) prematurely exhausted its finite reservoir of hydraulic fluid and the TVC flight control function became inoperable. The Castor 4B TVC actuators (provided by Allied Signal) were designed to operate for a finite number of nozzle steering 'push-pull' cycles. The actuators, which employed a blowdown system in which high-pressure helium gas was used to pressurize the hydraulic fluid tank, operated as specified. Each push-pull cycle of the TVC actuator consumed an increment of the on-board hydraulic fluid from the reservoir; the hydraulic fluid was actually dumped overboard after each cycle. The amount of hydraulic fluid stored in the reservoir was sized to accommodate the nominally predicted TVC steering profile with some hydraulic fluid margin in reserve.

Telemetry analysis revealed the Stage 1 motor TVC nozzle actuators were significantly 'over-cycled' starting shortly after liftoff in response to the TVC commands they received from the LQR controller. The post-failure investigation team pinpointed the source of the actuator over-cycling was an unanticipated low-frequency structural vibration mode that was not adequately filtered out in the TVC control loop compensation. The Conestoga TVC flight control system designers choose to employ a notch 'structural bending mode' digital filter in their loop compensation. A Bode gain and phase plot of a generic notch filter is shown in Figure 12 for reference and illustrative purposes. This notch filter was designed to deeply attenuate gain (i.e., filter out) the Conestoga launch vehicle's first structural bending mode vibrations in the rate gyroscope feedback signal to the TVC control law. The center frequency of the notch filter design was set at approximately 4 Hz in the frequency region where the structural Finite Element Model (FEM) predicted several closely spaced vehicle structural modes to occur during ascent. It is believed these were primarily torsional modes of the vehicle that were physically caused by the compliances between the strap-on Castor motors and the core vehicle. As it turned out the FEM of the launch vehicle structure grossly underestimated the first torsional mode of the system. The analysis of the ascent telemetry revealed the first torsional flexible mode was approximately 6.2 Hz.

Some background on bending mode filters is appropriate here before proceeding on. Notch filtering is a form of classical gain stabilization which provides attenuation of the control loop gain at a specifically desired frequency (typically either the first or second structural bending mode frequencies) so the so that stability is ensured regardless of the control loop phase uncertainty. It is not uncommon to include low-pass or notch bending mode filters in the flight control loops to attenuate the components of structural flexibility in the attitude/attitude rate sensor feedback signals so that the control law does not respond to potentially destabilizing flexible body effects. One general strategy for mitigating flexible body effects in flight control systems is the use of a low-pass filter for attenuating high-frequency bending modes in combination with a notch filter at specific low or mid-range frequencies closer to the flight control system bandwidth. In some cases the use of low-pass filter alone is sufficient. Unlike the notch filter, which ensures that a single specific bending mode in or very near the control bandwidth is not destabilized by feedback control, the low pass filter typically serves to rolloff the control system gain at frequencies above the control bandwidth. Generally speaking the notch filter creates less phase lag than the low-pass filter but the low-pass filter has the desirable feature of attenuating any high-frequency sensor noise or plant disturbance in the control loop. Neither form of control loop filtering introduces any active damping in the system.

Reference 16, published in 2001, is an analysis of fifty space failures through a systems engineering 'lens', attributes the Conestoga failure to two primary causes. According to Table I in Reference 16 the first cause of the Conestoga failure falls into the category of 'Design' and the second is in the category of 'Design Test & Verification'. The first failure cause category is defined as "fundamental defects or flaws in the design" while the second is defined as "inadequate test and verification process that allowed a latent design defect to remain uncorrected'. The identification, by the author of Reference 16, of 'Design' and 'Design Test & Verification' as the primary two causes of the Conestoga failure is credible as will become apparent in the remainder of this section.

It appears there were a number of TVC controller design cycles performed on Conestoga over a period of several years leading up to the launch. The stabilization and control of the rigid-body vehicle dynamics was relatively easily accomplished. Stabilization and control of the vehicles' flexible-body dynamics was a much more challenging task for the Conestoga TVC control system designer. Stability robustness was insufficient for the flexible body case. Early on in the initial design cycles, as alluded to above, a classical PID TVC control law approach was implemented. An attempt to phase stabilize the low frequency flexible modes was attempted. Various options were explored such as increasing the loop closure rate of the digital controller to decrease the phase lag due to the sampling process. However the PID design proved unable to handle the task of stabilizing the multiple closely spaced flexible modes of the launch vehicle structure in a frequency band around 4 Hz. The lack of frequency separation between the 4 Hz torsional modes relative to the desired PID control loop bandwidth proved an intractable situation for the control system designer. The PID control law approach was therefore abandoned in favor of a LQR controller design in tandem with notch filtering, centered at 4 Hz, of the vehicle's rate gyro feedback signal.

As mentioned above there was a significant mismatch between the as-designed center frequency of the Consestoga TVC control loop notch bending mode filter (4 Hz) and the actual as-flown vehicle torsional mode frequency that the filter was intended to 'notch out' (6.2 Hz). The successfully implementation of a notch filter is contingent on an accurate knowledge, to within say +/- 10%, of the specific bending mode frequency to be rejected from the feedback signal. If the actual bending mode frequency is lower (or higher) than predicted by modeling and analysis then the notch filter will be less stabilizing. It is for this reason control system designers typically only employ notch filters when absolutely necessary. The use of a notch filter on Conestoga most likely was the driver for high modal frequency accuracy, at least for the lower frequency flexible modes, in the launch vehicle structure FEM. It appears that a Ground Vibration Test (GVT) was performed on the Conestoga launch vehicle prior to launch. The Conestoga control system designer requested test-validated modal frequency, mode shape and modal damping data to complete his TVC control system synthesis. The control system designer suggested the performance of a 'hang and twang' type modal test in which the vehicle would be hung in air, via a suspension system of lightweight 'bungee' like cords to offload its mass, in order to approximate in Earth's 1-g environment the free-free boundary conditions experienced by the vehicle in flight. This would have most likely been a complex, time-consuming and costly form of GVT for Conestoga to perform but from a 20-20 hindsight perspective it appears that the 'hang and twang' test would likely have produced an accurate set of modal data for the control system designer's use.

The Conestoga GVT was instead performed on the launch vehicle while mounted on its launch pedestal at the pad. It also appears that the results of this GVT were then in turn used to validate the vehicle structure FEM. In the

validation process the analytic result from the FEM was compared with the modal data set taken during the GVT. The free-free FEM boundary conditions were adjusted to reflect the clamped-free test configuration of the Conestoga vehicle situated on its launch pedestal at the pad. A reasonably close match in flexible mode frequency was accomplished for only the first flexible mode; beyond the first mode of vibration the agreement between the FEM prediction and the GVT test data deteriorated significantly.,

What led to the significant mis-prediction (4 Hz vs. 6.2 Hz) in the vehicle's first torsional mode of vibration by the FEM structural model? This question remains unanswered, however, a consideration of the Conestoga's structure may shed some light on this question. The Conestoga launch vehicle was not a conventional long and slender 'stick shaped' rocket. It was a squat shaped core vehicle with several relatively large strap-on solid rocket motors attached by a complex system of mounting struts. These struts had spherical ball and socket type end fittings that most likely had some degree of joint 'play' in them. This type of physical strut arrangement could have introduced significant structural non-linear effect on the Conestoga vehicle. The degree to which the FEM picked up and accurately represented these non-linear strut end-fitting effects could be at the heart of the torsional mode frequency mis-prediction issue. Also the degree to which the Conestoga System Engineering team appreciated the potential for a non-linear structural response comes into consideration here as well. It could very well be that the team underestimated the technical challenge of developing a high-quality FEM of the Conestoga structure.

So what are the lessons to be learned from the Conestoga launch vehicle failure? It appears there are at least four lessons learned that can be taken away here that should be widely shared with the GN&C CoP:

Conestoga LL #1
Perform a Sensitivity Analysis of Notch Bending Mode Filter Performance
Notch filtering approaches for loop stabilization should be undertaken with great care and attention to modal data uncertainty. Consider Low Pass Filtering Approaches as an Alternative to Notch Filtering. If using a notch filter determine what the appropriate modal data accuracy tolerance is for the mission application at hand. Determine what happens if there is a mis-prediction in the bending mode frequency, or mode shape or mode damping, that exceeds that allowable tolerance.

Conestoga LL #2
Systems Engineering is Vitally Important to Mission Success
The System Engineering team should set the requirements for a Project's modeling and simulation activities and they should ensure FEM models are properly test-validated. System Engineering should understand the interplay between the GN&C and Structures disciplines, particularly in the area of Controls-Structures Interaction (CSI). Furthermore, the System Engineering team should develop an overall strategy and a detailed plan for a sufficiently rigorous test and verification process that will uncover and expose latent design defects. The employment of multiple independent verification analyses and tests should figure prominently in such a plan, particularly for a first-of-a-kind system development.

Conestoga LL #3
Define the Requirements for a Ground Vibration Test to Validate the Launch Vehicle Structural FEM
Define the requirements for FEM modal prediction accuracy and determine the type of GVT need to support FEM model validation.

Conestoga LL #4
If Developing a Unique One-of-a-Kind Vehicle Structure Perform Multiple Independent Structural Modeling and Analysis Cycles
Recognize and fully appreciate the technical challenges of modeling vehicles with a significantly different non-heritage type structural configuration. Anchor these structural modeling and analysis cycles with modal data from a GVT.

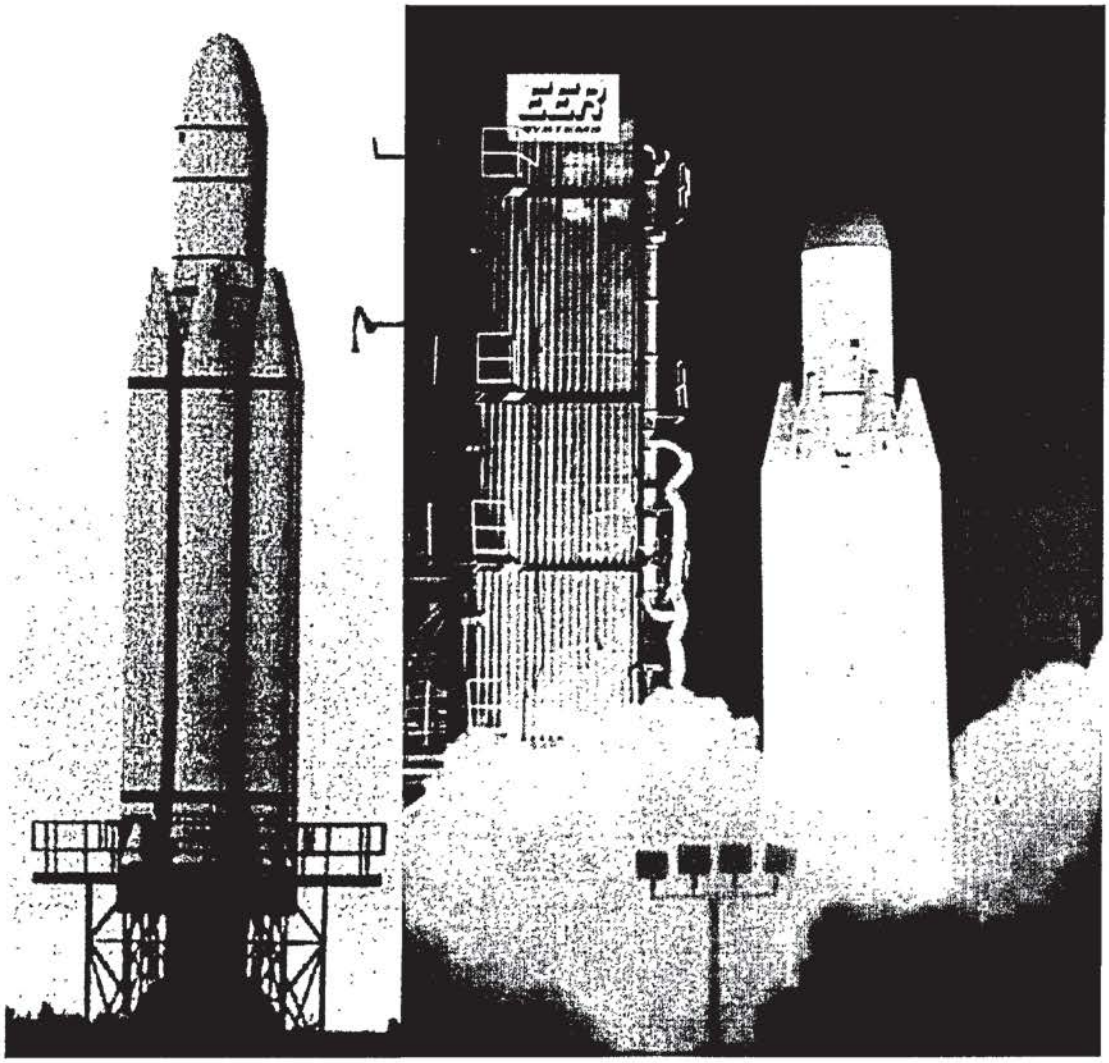

Figure 10. (a) Conestoga Launch Vehicle on Launch Pad at Wallops Island, (b) Liftoff of the Conestoga Launch Vehicle

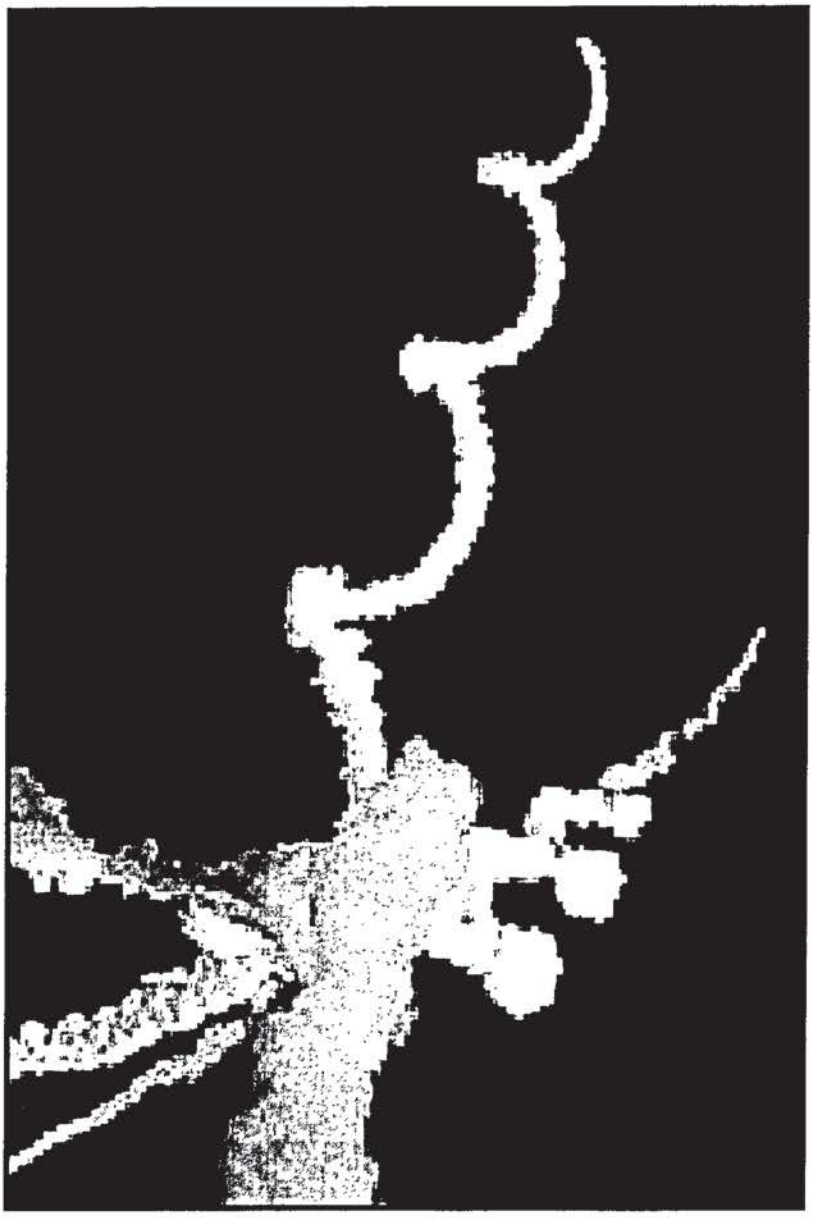

Figure 11. Conestoga Launch Vehicle Destruct at T+46 Seconds

$$H(s) = \frac{s^2 + 0.5s + 100}{s^2 + 5s + 100}$$

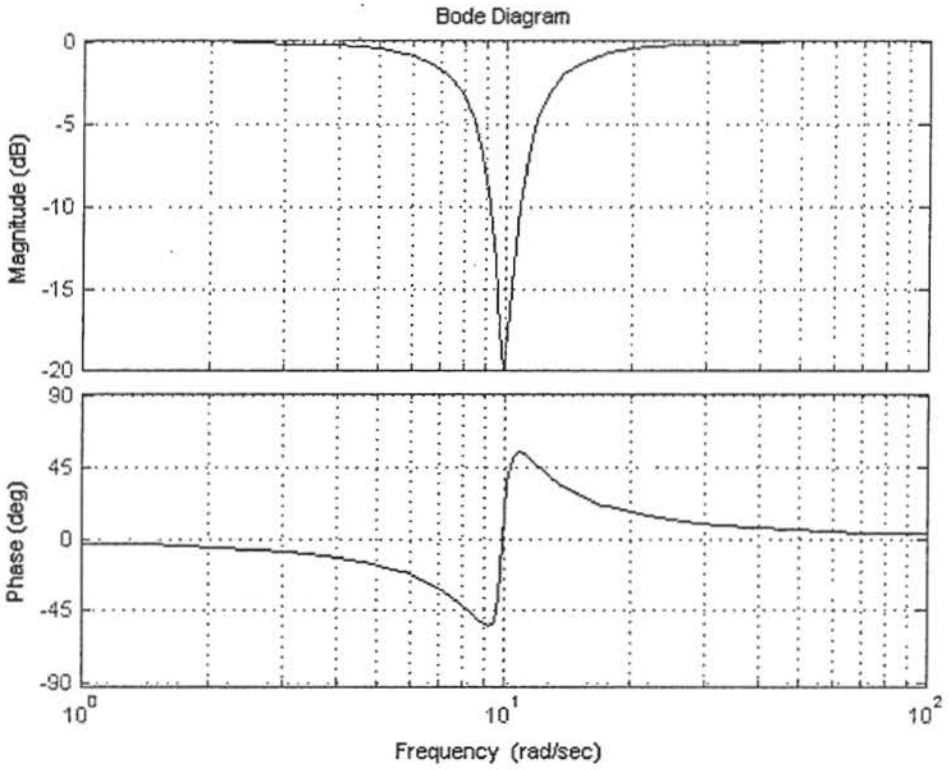

Figure 12. Generic Notch Bending Mode Filter

VI. Conclusions

This paper has focused on the fact that there have been important GN&C knowledge, in the form of lessons learned, that have been 'lost'. In the context of this paper "lost" refers to lessons that have not achieved broad visibility within the NASA-wide GN&C CoP because they are either undocumented, masked or poorly documented in the NASA Lessons Learned Information System. The capture and sharing of Knowledge across the Agency is not "nice to do" — it is "must do" responsibility for that NASA engineers and our industry partners. We need to take a look back to make sure we have comprehensively captured lessons from the past; this is especially important given the current demographics of NASA where a large percentage of senior NASA engineers are currently eligible for retirement. In order to avoid the loss of any more lessons it is recommended that at the conclusion of every significant engineering and research development the team involved should convene a sharing workshop to reflect on and capture its lessons learned. This shouldn't wait until after launch or closeout; it should take place immediately after the team has finished its major effort, while teams are still together and while their memories are still fresh in their minds. Utilizing an informal PaL session to explore what the team learned and what should the team change might be a preferred way to kick this process off.

The authors recommend that the GN&C engineering line organizations at each NASA Center make a good faith effort to look backwards in time to identify their individual critical lessons learned that have not yet been formally captured. Line managers should consider incentivizing those GN&C engineers that take the time to look back in time to identify and document "lost" lessons. While these important pieces of information may often times be commonly known conversational/oral 'tribal knowledge', the issue is that they have never been formally identified as such, documented and entered into the NASA LLIS for the benefit of others working on NASA Program/Projects, either as civil servants within the Agency or as employees of our industry partners. The authors would like to particularly recommend that a careful and detailed scrutiny of the Space Shuttle Program's (SSP) multi-decade collective GN&C design, development, test and operations experience be performed to identify any undocumented lessons learned that need to be captured. This retrospective look at the SSP GN&C history needs to be performed before the Program completely winds down and is terminated, an event which is now being planned for FY11.

Generally speaking most engineers need training on how to research and expoilt the appropriate lesson learned databases and document lessons learned. These same engineers need to be educated and trained in the ways of writing good lessons learned. The NASA LLIS should be consulted at the start of any new system development or research project. The multiple NEN online engineering Communities of Practice, such as the GN&C online engineering community, are excellent sources of discipline-specific knowledge and lessons. Engineering and Research organizations should be encouraged and empowered to initiate new or improve exisiting lessons learned research and documentation efforts. Internal and informal knowledge sharing workshops are a good grassroots approach to capturierng and disemninationg lesssons learned. Beyond those measures, Program and Project mansgers, together with thier Chief Engineers, need to continue to find ways to embed these lessons in NASA design & development processes. Some GN&C lessons learned may need to be formulated into engineering Recommended Best Practices. Critically important GN&C lessons that are continually being learned and re-learned should be established as policy.

The open sharing of in-house knowledge across the ten Centers is the only way NASA can become a true 'learning' organization. More visibility and cross-pollination of lessons is needed across all the Centers. Some possible methods to positively influnece the NASA learning process, adopted from Ref. 16, include the idea of generating a set of 'White Papers' that would provide synopses of lessons learned derived from flight system GN&C.engineering experiences. This idea could then be expanded into requiring GN&C system engineers and lead subsystem managers to take a daylong training module focusing on individual historic failure modes. Building on that, it would be highly informative to those managers to provide them follow-on training which addresses those particular systems failures that were casued by deleterious interactions between multiple subsystems or disciplines.

The X-38, Landsat-6, and Conestoga examples provided, along with the story of the B-2 stealth bomber crash in Guam, lead us to consider the following questions:

1) Do you work with systems or hardware that you do not understand?

2) How much do you need to know to do your job well?

3) How can your organization/program/project increase general understanding for all personnel?

4) How can your organization/program improve knowledge transfer?

5) How can your organization/program/project minimize the inevitable loss of experience and detailed system knowledge when an employee retires or leaves the program/project?

6) Consider that while many B-2 technicians were familiar with the pitot heat technique, only a few of their supervisors had heard of the workaround. What can be done to encourage communication both between peers and throughout the management hierarchy?

7) How do you determine when "tricks of the trade" are significant? How can you improve your processes for capturing and sharing those techniques?

In closing the authors would like to consider the B-2 stealth bomber crash again, this time to consider what the warning messages are for NASA from that particular failure scenario. At NASA, as in the Air Force, there is a need to continue to focus on capturing and transferring knowledge from personnel who work on complex systems and sophisticated hardware. The "Spirit of Kansas" accident investigation board had to talk to people who had not worked on the B-2 for ten years to find someone who completely understood how the aircraft functioned. As NASA transfers its hardware and software systems from one generation of engineers to the next, we need to ensure the current workforce also passes along their knowledge to their successors and leave detailed documentation for future personnel. The imminent rampdown and closure of the SSP will provide NASA with a challenging opportunity to demonstrate we are a learning organization that cares enough to invest the resources needed to sufficiently document the technical legacy of that outstanding and groundbreaking Program.

Acknowledgments

The authors would like to thank the GN&C Technical Discipline Team and line managers who have provided content and feedback on this topic. The lead author particularly wishes to acknowledge Steve Labbe (JSC) who provided the inspiration for this paper by referring to the X-38 'bent airframe' issue during a peer review discussion concerning the Max Launch Abort System (MLAS) aerodynamic uncertainty modeling. The detailed analysis results and other materials originally assembled by Steve Munday, Jeremy Hart, James Greathouse (all from JSC) were invaluable to the authors' understanding of the X-38 yawing moment IFA and the lessons learned to be extracted from the investigation of that rollover anomaly. The authors appreciate the insights and contribution of Mike Ruth (Orbital and a member of the NEC GN&C Technical Discipline Team) regarding the allocation of bandwidth in X-38 flight control system design. Mr. John Goodman (USA/ Houston) is recognized by the authors for his seemingly tireless efforts to not only document critically important GN&C lessons learned but also to provide his GN&C CoP colleagues at NASA and industry with practical guidance on the process and practice to effectively document lessons learned. Lastly, the authors would also like to thank Scott Glubke (GSFC Code 590 Chief Engineer) and Daria Topousis (JPL) for their thoughtful review and commentary of this paper.

References

1) *"Best Practices for Researching and Documenting Lessons Learned"*, NASA/CR–2008–214777, March 2008, John L. Goodman, United Space Alliance, Houston, TX

2) *"The Application of Best Practices to Unmanned Spacecraft Development: An Exploration of Success and Failure in Recent Missions"*, L. Sarsfield, RAND Corporation, Santa Monica, CA, 2000

3) "NASA: Better Mechanisms Needed for Sharing Lessons Learned", GAO-02-195, Government Accounting Office, January 2003

4) "Lessons Learned/ Knowledge Sharing Letter", NASA Chief Engineer/NASA Chief of Safety & Mission Assurance, 19 February 2009

5) "Exploiting Online Expertise and Knowledge Sharing for the Benefit of NASA's GN&C Community of Practice ", D. Topousis, C. J. Dennehy and K. Lebsock, AIAA paper, GN&C Conference, Toronto, Canada, 5 August 2010

6) *"NASA's Pause and Learn Process"* , NASA/GSFC Chief Knowledge Officer Brochure, http://www.nasa.gov/centers/goddard/pdf/284136main_PaL_Brochure_V4(c).pdf

7) "The Known Unknown", NASA Safety Center (NSC) System Failure Case Study Brochure, December 2008, Volume 2, Issue 09

8) Aviation Week, "Forgotten Lesson Caused B-2 Crash" June 6, 2008, http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/B-2060608.xml&headline=Forgotten%20Lesson%20Caused%20B-2%20Crash

9) *"X-38 Experimental Control Laws: Vehicle 131R Free Flights 1 & 2"*, Presentation to the SAE WAC, 11 September 2001, Steve Munday and Jeremy Hart, NASA/ JSC, GN&C Design and Analysis Branch

10) "34 Management Principles Employed in Configuration Management and Control in the X-38 Program" , NASA Document, Brian Anderson, 2004

11) *"The Landsat-6 Spacecraft: An Overview"*, Mowlem, E. W. and Dennehy, C. J., IEEE Aerospace and Electronic Systems Magazine, Volume 6, Issue 6, June 1991

12) Landsat-6 Failure Investigation, Final Report Summary, 16 January 1995, NOAA/Martin Marietta Corporation

13) *"Commercial Space Transportation Special Report: U.S. Small Launch Vehicles"*, 1st Quarter 1996, United States Department of Transportation, Federal Aviation Administration, Associate Administrator for Commercial Space Transportation, Washington, D.C. 20591

14) "Summary of Facts" USAF report, signed by Floyd L Carpenter Major General, USAF. President of the Accident Investigation Board.

15) "Statement of Opinion B2A, T/N 89-0127 Accident 23 February 2008" USAF report, signed by Floyd L Carpenter Major General, USAF. President of the Accident Investigation Board.

16)" Failure-Space: A Systems Engineering Look At 50 Space System Failures", J. Steven Newman, National Aeronautics and Space Administration, Washington, DC 20546, Acta Astronautica Vol. 48. No 5-12. pp. 517-527. 2001